UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/085,457	02/27/2002	Sonja Buchegger	CH920010040US1	1821

7590 09/30/2005

IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. BOX 218 - 39 -254
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
HENEGHAN, MATTHEW E	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 09/30/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/085,457	BUCHEGGER, SONJA	
	Examiner	Art Unit	
	Matthew Heneghan	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 February 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 February 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

AT

DETAILED ACTION

1. Claims 1-26 have been examined.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(1) because the reference characters and labels in figures 1-15 are not completely legible.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: figure 3, item 230; figure 5, items 420 and 440; and figure 14, items 231 and 232.

4. Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be

notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

5. Claims 3, 5, 8, 10, 13, 15, 19, 21, 24, and 26 are objected to because of the following informalities: The word "incrementing" has multiple definitions within the art and it is not clear, in light of the instant specification, which definition should be applied. This word may be construed as meaning "increasing the value of a variable by exactly one" or, alternatively, "increasing the value of a variable by any amount." For purposes of the prior art search, the latter definition is being applied. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 4, 5, 9, 10, 14, 15, 20, 21, 25, and 26 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Each claim recites the limitation "the other node." There is insufficient antecedent basis for this limitation in the claim. It is being presumed that this refers to "another node" in the first limitation of each claim.

Claims 5, 10, 15, 21, and 26 depend from rejected claims 4, 9, 14, 20, and 25, respectively, and include all the limitations of those claims, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1, 3-6, 8-11, 13-17, 19-22, and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,321,338 to Porras et al. in view of U.S. Patent No. 5,475,838 to Feshkens et al.

Regarding claims 1, 6, and 11, Porras discloses a hierarchical network surveillance system wherein domain monitors are used to monitor events sent to them by each of the service monitors in their respective domains, each of which constitutes a neighbor in the domain monitor's neighborhood (see column 3, line 42 to column 4, line

18). Received events are subjected to security tests performed by the monitor's analysis engine, potentially triggering remedial action, such as the sending of a alarm to nodes on a subscription list (see column 11, line 12 to column 12, line 29).

Porras does not disclose the maintaining and modifying of network topology data.

Feshkens discloses the maintaining of topology data and the changing of that data in response to control modules (monitors) being added or removed (see column 7, lines 46-54). Feshkens further suggests that this is done because such systems are challenging to manage and the management functions must adapt to new management requirements of the system.

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Porras by maintaining and modifying topology data, as disclosed by Feshkens, as the management functions must adapt to new management requirements of the system.

Regarding claims 3, 8, and 13, Porras further discloses that a statistical algorithm employed by the monitor that tests the number of event occurrences, described as the distance between the short-term and long-term statistics, over a short-term period against a score threshold derived from long-term statistics, producing a score (i.e. a rating) in order to determine an anomalous event (see column 6, lines 38-67).

Porras does not disclose an incrementing algorithm in determining the score.

Official notice is given that it is well-known in the art to use mathematical addition (i.e. incrementing) in the determination of the distance between two numbers (e.g. X = Y + (-Z)), as this is an efficient method for performing a comparison in linear space.

Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to implement the determination of the distance between two numbers using an algorithm that incorporates incrementation, as this is an efficient method for performing a comparison in linear space.

Regarding claims 4, 5, 9, 10, 14, and 15, Porras discloses the use of an enterprise monitor that receives events from domain monitors that have originated with service monitors (see column 4, lines 19-47). The events are handled by the enterprise monitors in a manner similar to the domain monitors. Handlers may be invoked to validate the integrity of network services to ensure that privileged services have been subverted (i.e. the node passing on the event and generating the alarm is trusted) and may sever channels (modify the topography) as necessary (see column 12, lines 7-19).

Regarding claims 16, 17, 19-22, and 24-26, the topology data must necessarily be stored in memory.

7. Claims 2, 7, 12, 18, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,321,338 to Porras et al. in view of U.S. Patent No. 5,475,838 to Feshkens et al. as applied to claims 1, 6, 11, 17, and 22 above and further in view of U.S. Patent No. 5,414,833 to Hershey et al.

Though both the inventions of Porras and Feshkens are capable to sending an alarm to all nodes, each only discloses the sending of alarms to selected nodes according to a rule, without specifically suggesting a rule for a broadcasting of an alarm.

Hershey discloses the broadcasting of an alert to all nodes in order to inform all users that a virus has been detected (see column 19, lines 33-44).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention of Porras and Feshkens by broadcasting of an alert to all nodes, as disclosed by Hershey, in order to inform all users that a virus has been detected.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,777,549 to Arrowsmith et al. discloses a system for policy-based alarm notification.

U.S. Patent No. 5,991,881 to Conklin et al. discloses a network surveillance system that sends alarms.

U.S. Patent No. 6,301,668 to Gleichauf et al. discloses system for using network topologies in vulnerability assessments.

U.S. Patent No. 6,519,703 to Joyce discloses a system employing heuristics to determine trust among system nodes.

U.S. Patent No. 6,574,737 to Kingsford et al. discloses a vulnerability assessment tool.

U.S. Patent No. 6,775,657 to Baker discloses a layered intrusion detection system.

U.S. Patent No. 6,930,978 to Sharp et al. discloses a sniffer testing for traffic thresholds in intrusion detection.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew E. Heneghan, whose telephone number is (571) 272-3834. The examiner can normally be reached on Monday-Friday from 8:30 AM - 4:30 PM Eastern Time.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
P.O. Box 1450
Alexandria, VA 22313-1450
Or faxed to:
(571) 273-3800

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MEH

September 27, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100